ABUSING BROWSER USER INTERFACES FOR FUN & PROFIT
HELLO

MY NAME IS Rosario

sites.google.com/site/tentacoloviola/
Socially Engineered Malware

2012 Facts

200K New Malware Samples Every Day

1.5+ Billions Malware Attacks Originated From The Web

Mostly Originated By User Initiated Downloads
• GUIDANCE WHILE SURFING THE WEB

• PROTECTION FROM MALICIOUS SITES

• RELIABLE BROWSER SECURITY MECHANISMS
ENHANCED MEMORY PROTECTION TECHNOLOGIES FOR PROTECTING AGAINST EXPLOITS AND DRIVEBY DOWNLOADS (ASLR, DEP, GS, ETC)

EMBEDDED SECURITY FILTERS AGAINST WEB ATTACKS (XSS FILTER, ANTI FRAMING/CYCKJACKING, ETC)

MALWARE/PHISHING RECOGNITION TECHNOLOGIES (SAFE BROWSING, SMARTSCREEN FILTER, ETC)

TRUSTED AND RECOGNIZABLE USER INTERFACES TO HELP USERS IN MAKING AWARE CHOICES WHILE SURFING THE WEB
URL OBfuscATION FLAWS

- EXPLOIT A DESIGN FLAW IN BROWSERS THAT ARE NOT ABLE TO RELIABLY RENDER THE URL REQUIRED BY THE USER
- URL FORMAT FollowS THE GENERAL PATTERN http://username:password@mysite.com WITH OPTIONAL password FIELD
- http://www.bankofamerica.com&service=...@174.120.41.176/~inferno/exploits/obfusurl/index.htm

RAISE A WARNING

DISABLES RESOLUTION FOR URLs WITH EMBEDDED CREDENTIALS

RENDERS PAGE AND STRIPS CREDENTIALS FROM THE URL AND REVEALING TRUE NATURE OF THE DOMAIN
DOWNLOAD DIALOG SPOOFING

• VICTIM VISITS ROGUE WEBSITE

• WEBSITE IMMEDIATELY SPAWNS A NEW NAVIGATION WINDOW LINKING TO A BENIGN WEBPAGE

• ROGUE WEBSITE SETS THE NEW NAVIGATION WINDOW URL TO A RESOURCE SERVED WITH Content-Disposition: attachment HEADER

• A DOWNLOAD NOTIFICATION BAR/DIALOG APPEARS IN THE CONTEXT OF THE NEW NAVIGATION WINDOW

• VICTIM IS TRICKED TO BELIEVE DOWNLOAD HAS BEEN ORIGINATED FROM THE BENIGN WEBSITE

http://1camtu.coredump.cx/fdl/
BROWSER SECURITY NOTIFICATIONS

- CRUCIAL PART OF THE BROWSER TRUST MODEL
- NOTIFY USERS BEFORE MAKING IMPORTANT CHOICES
- COMMUNICATION MEDIUM BETWEEN USERS AND BROWSERS
- NEED TO BE RECOGNIZABLE AND TRUSTED
MODAL NOTIFICATIONS

STRONG VISUAL CONTRAST • GRAB USER ATTENTION • BLOCK WORKFLOW

OS GENERATED

- IMPORTANT NOTIFICATIONS ONLY
- NOT STRICTLY PART OF CHROME
- DEFAULT ANSWER PROBLEM

BROWSER GENERATED

- TRIGGERED IN SEVERAL SCENARIOS
- SOMETIMES CAN BE VERY ANNOYING
- DEFAULT ANSWER PROBLEM
MODELESS NOTIFICATIONS

- Designed to inform user without interrupting navigation
- Stay in context of the navigation window
- Chrome NOT DOM

FILE DOWNLOADING  HTML5 APIs

PLUGINS ACTIVATION
MODAL TO MODELESS SHIFT

MODELESS   MODELESS   MODELESS   MIXED   MODAL

MODELESS   MODELESS   MODELESS   MODAL   MODAL

MODAL   MODAL   MODAL   MODAL   MODAL

MODELESS   MODELESS   MODELESS   MODELESS   MODAL

EXTENSIONS/ADDONS
4 PROBLEMS ABOUT MODELESS NOTIFICATIONS
1. DISPLAYED EVEN IF THE WINDOW IS IN BACKGROUND

2. KEYBOARD SHORTCUTS ENABLED FOR NOTIFICATION BARS

3. NOTIFICATION BARS CAN BE Navigated USING TAB KEY

4. NOTIFICATION BARS ARE BOUND TO THE NAVIGATION WINDOW
NOTIFICATIONS IN BACKGROUND WINDOWS

SCENARIO:
1. USER BROWSES ON ATTACKER WEBSITE
2. WEB PAGE SPAWNS A POPUP WINDOW
3. POPUP IS OPENED ON THE BACKGROUND (POPUNDER)
4. ON WINDOWS 7/8 THE POPUNDER IS MERELY UNNOTICED
5. POPUNDER INITIATES A DOWNLOAD
6. MODELESS NOTIFICATION IS TRIGGERED (HIDDEN FROM USER VIEW)
7. POPUNDER TAB DOESN’T BLINK TO GIVE EVIDENCE OF A PENDING NOTIFICATION
KEYBOARD SHORTCUTS

- ARE AVAILABLE FOR ACTIVATING ACTIONS ON NOTIFICATION BARS
- IE ALLOWS THIS FOR FILE DOWNLOAD NOTIFICATIONS
  - ALT + R • ALT + S • ALT + O
- IE & FF ALLOW THIS FOR HTML5 API NOTIFICATIONS
  - ALT + O
  - ALT + A • ALT + O
- NAVIGATION WINDOW NEEDS TO BE FOCUSED FOR USING SHORTCUTS
USING TAB IN NOTIFICATION BARS

SOME BROWSERS ALLOW USING TAB KEY TO NAVIGATE ON NOTIFICATION BARS

- IE ALLOWS THIS FOR FILE DOWNLOAD NOTIFICATION

Do you want to run or save CosmicBreak_BR_setup.exe (1.18 MB) from tentacoloviola.altervista.org?

- CHROME SKIPS THE FILE OPENING BUTTON

NOTIFICATION BAR IS PART OF CHROME: NO NAVIGATION USING DOM EVENTS IS ALLOWED
BOUND TO NAVIGATION WINDOW

AS THEY ARE BUILT IN CHROME, NOTIFICATION BARS CAN BE:

- MOVED AROUND THE SCREEN ALONG WITH THE NAVIGATION WINDOW
- RESIZED ALONG WITH THE NAVIGATION WINDOW
- CLOSED TOGETHER WITH THE NAVIGATION WINDOW
- ALSO BOUND TO ORIGINATING DOMAIN
ATTACK SCENARIO #1

1. USER BROWSES ON ATTACKER WEBSITE
2. WEB PAGE SPAWNS A POPUNDER WINDOW
3. ON WINDOWS 7/8 THE POPUNDER IS MERELY UNNOTICED
4. POPUNDER INITIATES A DOWNLOAD OF A .EXE FILE
5. MODELESS NOTIFICATION IS TRIGGERED (HIDDEN FROM USER VIEW)
6. POPUNDER TAB DOESN’T BLINK TO GIVE EVIDENCE OF A PENDING NOTIFICATION
7. AFTER NOTIFICATION IS READY, POPUNDER IS STILL IN BACKGROUND BUT HAS THE FOCUS!
8. EVERY KEYBOARD INPUT WILL BE DIRECTED TO THE POPUNDER...
9. USER ENTERS “TAB” + “R” or “SPACE” or “ENTER”
10. CODE EXECUTION WITHOUT ANY NOTIFICATION OR USER CONFIRMATION
ATTACK SCENARIO #1 - BONUS

- IN IE9 OPENING POPUNDER WINDOW USING:

```html
<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7" />
```

**WILL BRING THE FOCUS OF THE POPUNDER DIRECTLY ON THE NOTIFICATION BAR**

- **THIS MEANS YOU CAN TRIGGER CODE EXECUTION BY JUST TYPING A KEY:**
  - R key (key changes according to OS language)
  - SPACE key
  - ENTER key
LIMITATIONS FOR ATTACK #1

1. SMARTSCREEN FILTER
2. USER ACCESS CONTROL
MALICIOUS DOWNLOAD PROTECTIONS

BLOCKING ACCESS TO MALICIOUS URLS & FILES BEFORE LOADING THE CONTENT

FUNCTIONAL COMPONENTS:

- A CLOUD REPUTATION-BASED SYSTEM
- SCOURS THE WEB FOR MALWARE
- CATEGORIZES FILES USING BLACKLISTS
- ASSIGNS FILES A SCORE

- A BROWSER AGENT
- REQUESTS INFORMATION FROM THE CLOUD
- PROVIDES FEEDBACKS ABOUT DOWNLOADED FILES
- ENFORCES WARNING/BLOCKING FUNCTIONS
IMPLEMENTATIONS

SAFE BROWSING

- Based on Google Safe Browsing API v.2
- Supports URL reputation
- Application reputation (Chrome only)

SMARTSCREEN FILTER

- Introduced in IE8
- Supports app reputation since IE9
- System wide extension in Windows 8

CHARTS FROM NSS LABS REPORT 2012
**SMARTSCREENFILTER**

**INPUT:** IP • URL • FILE HASH (SHA256) • FILENAME (BASE64) • SIGNING CERTIFICATE (if available)

**OUTPUT:**

- Do you want to run or save thebat_home_4-2-42.msi (6.87 MB) from fs13.fliehippo.com?
  - Run
  - Save
  - Cancel

- malware.zip is unsafe to download and was blocked by SmartScreen Filter. Learn more
- View downloads

- 02-FHU-IVU.exe is not commonly downloaded and could harm your computer.
  - Delete
  - Actions
  - View downloads

- SUCCEEDED
- BLACKLISTED
- REPUTATION FAILURE

Bar color changes according to the **SIGNING CERTIFICATE** + CHECK RESULT
REPUTATION CHECK IS NOT 100% RELIABLE
MORE THAN 20% SAMPLES ON
http://minotauranalysis.com/exetweet/default.aspx WILL PASS THROUGH

BUY AN **EV** CERTIFICATE AND GAIN REPUTATION!
NEWLY PUBLISHED EXECUTABLES SIGNED WITH AN **EV** CERTIFICATE WILL IMMEDIATELY ESTABLISH A GOOD REPUTATION EVEN IF NO PRIOR REPUTATION EXISTS

RESPONSE TIME FOR CATCHING NEW EXECUTABLE SAMPLES ALLOWS FOR EASY BYPASS IN THE FIRST PUBLISHING DAYS

INTERNET CONNECTION NEEDED FOR PERFORMING THE CHECK (more on this later...)
ATTACK SCENARIO #10 ON STEROIDS

MITM SCENARIO

1. ATTACKER SETS UP A FREE ACCESS POINT
2. BLOCKS COMMUNICATIONS TO SMARTSCREEN SERVER
3. RESULT IS:

4. TRICK VICTIM TO TYPE “R”/ ”Enter” / ”Space” ONCE AGAIN...
5. ARBITRARY CODE EXECUTION!
USER ACCESS CONTROL

ONLY TRIGGERED WHEN ADMINISTRATIVE PRIVILEGES ARE REQUIRED

YOU CANNOT BYPASS THAT. FULL STOP.

DO YOU REALLY NEED THAT FOR CAUSING SERIOUS TROUBLES? ASK ZEUS / CARBERP...
LIMITATIONS FOR ATTACK #1 REVISITED

1. SMARTSCREEN FILTER ✗
2. USER ACCESS CONTROL → Not a problem
ATTACK SCENARIO #2

DYNAMIC WINDOW OVERLAY

1. USER BROWSES ON ATTACKER WEBSITE
2. WEB PAGE SPAWNS A POPUNDER WINDOW AT SOME GIVEN COORDINATES
3. POPUNDER INITIATES A DOWNLOAD OF A .EXE FILE
4. MODELESS NOTIFICATION IS TRIGGERED (HIDDEN FROM USER VIEW)
5. POPUNDER TAB DOESN’T BLINK TO GIVE EVIDENCE OF A PENDING NOTIFICATION
6. ATTACKER TRICKS VICTIM TO CLICK ON A GIVEN LINK/BUTTON
7. PAGE IS LISTENING ON MOUSE MOVES
8. AS SOON AS THE MOUSE IS HOVERING ON THE BUTTON, WINDOW IS CLOSED
9. IF TIMING IS APPROPRIATE THERE ARE GOOD CHANCES OF VICTIM CLICKING ON THE UNDERLYING POPUNDER
ATTACK SCENARIO #2 RELOADED

- EVERY TIME A FILE IS DOWNLOADED FROM THE WEB THE OS ADDS A ZONE INFORMATION FILE TO THE DISK
- ZONE INFORMATION FILE IS WRITTEN IN AN ASD (alternate data stream)
- IT CONTAINS A REFERENCE TO THE SECURITY ZONE THE FILE WAS DOWNLOADED FROM (e.g. INTERNET)

- LAUNCHING AN UNKNOWN .EXE FILE DOWNLOADED FROM THE WEB WILL Prompt A CONFIRMATION DIALOG, NOT BYPASSABLE

- A SMARTSCREEN CHECK IS PERFORMED (BUT YOU ALREADY KNOW HOW TO BYPASS IT)
- NO FURTHER DIALOGS ARE DISPLAYED
- CODE EXECUTION!
ATTACK SCENARIO #2.b

DYNAMIC WINDOW OVERLAY

1. USER BROWSES ON ATTACKER WEBSITE
2. WEB PAGE SPAWNS A POPUNDER WINDOW AT SOME GIVEN COORDINATES
3. POPUNDER LOADS A WEBPAGE REQUIRING SOME PRIVILEGES (e.g. YOUR POSITION)
4. MODELESS NOTIFICATION IS SHOWN (HIDDEN FROM USER VIEW)
5. POPUNDER TAB DOESN’T BLINK TO GIVE EVIDENCE OF A PENDING NOTIFICATION
6. ATTACKER TRICKS VICTIM TO CLICK ON A GIVEN LINK/BUTTON
7. PAGE IS LISTENING ON MOUSE MOVES
8. AS SOON AS THE MOUSE IS HOVERING ON THE BUTTON, WINDOW IS CLOSED
9. IF TIMING IS APPROPRIATE THERE GOOD CHANCES THE VICTIM CLICKS ON THE UNDERLYING POPUNDER
ATTACK SCENARIO #2.

DYNAMIC WINDOW OVERLAY

1. USER BROWSES ON ATTACKER WEBSITE
2. WEB PAGE SPAWNS A POPUNDER WINDOW AT SOME GIVEN COORDINATES
3. POPUNDER LOADS A WEBPAGE SERVED WITH X-FRAME-OPTIONS (e.g. TWITTER)
4. ATTACKER TRICKS VICTIM TO CLICK ON A GIVEN LINK/BUTTON
5. PAGE IS LISTENING ON MOUSE MOVES
6. AS SOON AS THE MOUSE IS HOVERING ON THE BUTTON, WINDOW IS CLOSED
7. IF TIMING IS APPROPRIATE THERE GOOD CHANCES THE VICTIM CLICKS ON THE UNDERLYING POPUNDER
SOME PROPOSALS

1. Notifications on background windows are useless (at best). **Let the notification pops-up after some seconds since the window has regained focus**

2. Disable Tab key in the notification bar, just use the mouse. If you are concerned about accessibility enable complex keyboard shortcuts in order to limit the chance of being social engineered.

3. Some sensitive notifications (e.g. file downloading) should be ever kept in a static frame of the chrome, not bound to navigation window.

4. Browser initiated switches between windows of different domains should be combined with a graphical effect (e.g. fading, etc) in order to give users adequate reaction time.
CONCLUSIONS

1. The browsers shift from modal to modeless notifications is still not mature.

2. Implementations are not secure enough to protect users' safety: at least two techniques allow for stealth remote code execution.

3. Why try to build complex and unreliable exploits if getting code execution is simple like pressing one key? 😊